UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,860	04/28/2006	Leeor Aharon	1893/45	3794

44696 7590 12/24/2009

DR. MARK M. FRIEDMAN
C/O BILL POLKINGHORN - DISCOVERY DISPATCH
9003 FLORIN WAY
UPPER MARLBORO, MD 20772

EXAMINER	
PEARSON, DAVID J	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
12/24/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mark_f@friedpat.com
nomi_m@friedpat.com
friedpat.uspto@gmail.com

Office Action Summary	Application No.	Applicant(s)	
	10/577,860	AHARON ET AL.	
	Examiner	Art Unit	
	DAVID J. PEARSON	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14 and 16-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14 and 16-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

1. Claims 1, 11, 16-17 and 20 have been amended. Claim 15 has been canceled. Claims 23-26 are newly added. Claims 1-14 and 16-26 have been examined.

Response to Arguments

2. Applicant's arguments filed 09/24/2009 in regards to the 35 USC 101 rejection of claims 20-22 have been fully considered but they are not persuasive.

Applicant's arguments with respect to claims 1, 11, 16-17 and 20 have been considered but are moot in view of the new ground(s) of rejection.

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 101

4. Claims 20-22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 20-22 are directed towards "an apparatus". However the components of the "apparatus" are "a filter apparatus", "a disassembler", "an assembly instructions analyzer" and "a vulnerable return address detector" are show in the drawings and in the Specification as software modules (note Fig. 4, Specification page 5, lines 28-29). Therefore the claimed "apparatus" is composed entirely of software and is therefore non-statutory subject matter.

Examiner recommends amending claim 20 to include hardware components (processor, program storage device) as similarly found in claim 17 to make all embodiments of claim 20 statutory. Note MPEP 2106.01 for guidance on computer related statutory subject matter.

Claim Rejections - 35 USC § 103

5. Claims 1, 3-4, 10 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti (U.S. Patent 7,389,540; hereafter "Radatti"), and further in view of Szor (U.S. Patent 7,293,290) and Schmall ("Classification and identification of malicious code based on heuristic techniques utilizing Meta languages").

For claims 1 and 20, Radatti teaches a method and apparatus for detecting malicious code in a stream of data traffic input to a gateway of a data network, the method comprising the steps of:

(a) monitoring by the gateway for at least one suspicious portion of data in **a portion of** the stream of data traffic (note column 5, lines 52-65).

Radatti differs from the claimed invention in that they fail to teach:

Data traffic **that is expected to lack executable code**.

Szor teaches:

Data traffic **that is expected to lack executable code** (note column 2, lines 13-21).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the scanner of Radatti with the scanning selected ports for executable code for further analysis of Szor. One of ordinary skill in the art would have been motivated to combine Radatti and Szor because executable code normally does not appear on certain ports and is therefore suspicious when it is present (note column 2, lines 13-21 of Szor).

The combination of Radatti and Szor differs from the claimed invention in that they fail to teach:

(b) upon detecting said at least one suspicious portion of data, attempting to disassemble said at least one suspicious portion of data thereby attempting to produce disassembled code;

Wherein for each instruction in said disassembled code,

(c) assigning respectively a threat weight for each said instruction; and

(d) accumulating said threat weight to produce an accumulated threat weight.

Schmall teaches:

(b) upon detecting said at least one suspicious portion of data, attempting to disassemble said at least one suspicious portion of data thereby attempting to produce disassembled code (note page 149, "disassembler/emulator");

Wherein for each instruction in said disassembled code,

(c) assigning respectively a threat weight for each said instruction (note page 146, "A heuristic engine based on a weight based system…"); and

(d) accumulating said threat weight to produce an accumulated threat weight (note page 146, "A heuristic engine based on a weight based system…").

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Radatti and Szor and the disassembler/weight based analyzing system of Schmall. It would have been obvious because a simple substitution of one known element (disassembler/weight based analyzing of Schmall) for another (pattern matching of Radatti) would yield the predictable results of identifying malicious code.

For claim 3, the combination of Radatti, Szor and Schmall teaches claim 1, wherein said monitoring is performed by skipping acceptable data in the stream of data traffic, said acceptable data being consistent with a protocol used by the data stream (note column 5, lines 52-65 of Radatti and column 4, lines 14-19 of Szor).

For claim 4, the combination of Radatti, Szor and Schmall teaches claim 3, wherein said acceptable data includes acceptable executable code (note column 5, lines 52-65 of Radatti and column 4, lines 14-19 of Szor).

For claim 10, the combination of Radatti, Szor and Schmall teaches claim 1, wherein the stream of data traffic includes an encoded data portion, further comprising the step of, prior to said attempting to disassemble:

(e) decoding said encoded data portion (note page 149, "… normalize the given input file..." of Schmall).

6. Claims 11 and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Radatti, Szor and Schmall as applied to claim 1 above, and further in view of Muttik (U.S. Patent 6,775,780).

For claims 11 and 16-17, the combination of Vella and Schmall teaches a method, program storage device and system for detecting malicious code in a stream of data traffic input to a gateway of a data network, the stream of data traffic including data packets, the method comprising the steps of:

(a) monitoring by the gateway for at least one suspicious portion of data in **a portion of** the stream of data traffic (note column 5, lines 52-65 of Radatti) **that is expected to lack executable code** (note column 2, lines 13-21 of Szor);

(b) upon detecting said at least one suspicious portion of data, attempting to disassemble said at least one suspicious portion of data thereby attempting to produce disassembled code (note page 149, "disassembler/emulator" of Schmall).

Wherein for each instruction in said disassembled code,

(c) assigning respectively a threat weight for each said instruction (note page 146, "A heuristic engine based on a weight based system…" of Schmall); and

(d) accumulating said threat weight to produce an accumulated threat weight (note page 146, "A heuristic engine based on a weight based system…" of Schmall).

The combination of Radatti, Szor and Schmall differs from the claimed invention in that they fail to teach:

wherein said threat weight for each said instruction is selectively either:

(i) increased for a legal instruction, and

(ii) decreased for an illegal instruction.

Muttik teaches:

wherein said threat weight for each said instruction is selectively either:

(i) increased for a legal instruction (note column 5, lines 14-21), and

(ii) decreased for an illegal instruction (note column 5, lines 14-21).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Radatti, Szor and Schmall and the negative

and positive weights of Muttik. It would have been obvious because a simple substitution of one known element (negative and positive weights of Muttik) for another (weights only for suspicious activity of Schmall) would yield the predicable results of identifying malicious code (note column 5, lines 20-21 of Muttik).

7. Claims 2, 6-7 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Radatti, Szor, Schmall and Muttik as applied to claims 1 and 11 above, and further in view of Shipley (U.S. Patent 6,119,236).

For claim 2, the combination of Radatti, Szor and Schmall differs from the claimed invention in that they fail to teach:

Wherein said at least one suspicious portion of data contains at least one illegal character in a protocol of the stream of data traffic.

Shipley teaches:

Wherein said at least one suspicious portion of data contains at least one illegal character in a protocol of the stream of data traffic (note column 6, lines 40-46).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Radatti, Szor and Schmall and the protocol monitoring of Shipley. It would have been obvious because combining prior art elements according to known methods would yield the predictable results of identifying an intrusion attempt (note column 6, lines 45-46 of Shipley).

For claim 6, the combination of Radatti, Szor, Schmall and Shipley teaches claim 1, further comprising the step of:

(e) upon said accumulated threat weight exceeding a previously defined threshold level, performing an action selected from the group of:

(i) generating an alert (note page 146 of Schmall), and

(ii) blocking traffic from the source of the suspicious data (note column 8, lines 5-8 of Shipley).

For claim 7, the combination of Vella, Schmall and Shipley teaches claim 6, wherein said blocking is solely in the stream of data traffic (note column 8, lines 5-15 of Shipley).

For claim 14, the combination of Radatti, Szor, Schmall, Muttik and Shipley teaches claim 11, further comprising the steps of:

(e) receiving the data packets input from a wide area network interface of the gateway, thereby building the packets into a virtual stream inside the gateway (note column 5, lines 24-31 of Shipley); and

(f) upon said accumulated threat weight exceeding a previously defined threshold level, performing an action selected from the group of:

(i) generating an alert (note page 146 of Schmall), and

(ii) blocking traffic from the source of the suspicious data (note column 8, lines 5-8 of Shipley).

8. Claims 5, 8-9, 12-13, 18-19 and 21-22 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Radatti, Szor, Schmall and Muttik as applied to claims 1, 11, 17 and 20 above, and further in view of Made (U.S. Patent Application Publication 2002/0056076).

For claim 5, the combination of Radatti, Szor and Schmall differs from the claimed invention in that they fail to teach:

wherein upon reaching a branch in said disassembled code, further accumulating said threat weight respectively for each branch option in said disassembled code, thereby producing said accumulated threat weight for each said branch option.

Made teaches:

wherein upon reaching a branch in said disassembled code, further accumulating said threat weight respectively for each branch option in said disassembled code, thereby producing said accumulated threat weight for each said branch option (note paragraph [0042]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Radatti, Szor and Schmall and analyzing both

sides of a branch of Made. One of ordinary skill in the art would have been motivated to combine Radatti, Szor, Schmall and Made because analyzing both portions of a branch would provide a more thorough analysis of the executable program.

For claims 8, 12, 18 and 21, the combination of Radatti, Szor, Schmall, Muttik and Made teaches claims 1, 11, 17 and 20, wherein said attempting to disassemble is initiated at a plurality of initial instructions, each of said initial instructions with a different offset within said at least one suspicious portion of data, and said threat weight is accumulated respectively for each said offset (note paragraph [0042] of Made).

For claims 9, 13, 19 and 22, the combination of Radatti, Szor, Schmall, Muttik and Made teaches claims 1, 11, 17 and 20, wherein said attempting to disassemble is initiated at an initial instruction of an address of previously known offset relative to a vulnerable return address (note paragraph [0042] of Made).

9. Claims 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Radatti, Szor, Schmall, Muttik and Made as applied to claims 8, 12, 18 and 21 above, and further in view of Szor (U.S. Patent Application Publication 2004/0015712; hereafter '712).

For claims 23-26, the combination of Radatti, Szor, Schmall, Muttik and Made differs from the claimed invention in that they fail to teach:

Wherein said attempting to disassemble is initiated at every offset within said at least one suspicious portion of data.

'712 teaches:

Wherein said attempting to disassemble is initiated at every offset within said at least one suspicious portion of data (note paragraph [0054]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the combination of Radatti, Szor, Schmall, Muttik and Made and the multiple offsets of '712. One of ordinary skill would have been motivated to combine Radatti, Szor, Schmall, Muttik, Made and '712 because there are many entry points a virus can begin from (note paragraph [0052] of '712).

Response to Arguments

10. Applicant argues claims 20-22 are statutory subject matter (note Remarks, page 11).

Examiner disagrees. As applicant notes claims 20-22 have both software and hardware embodiments (note Remarks, page 11). While the hardware embodiments are statutory, the software embodiments are functional descriptive material and therefore non-statutory (note MPEP 2106.01). Claims 20-22 are non-statutory because

not all of their embodiments are statutory subject matter. As noted above, Examiner recommends amending claims 20-22 to include hardware components, which would make all embodiments of claims 20-22 statutory.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Szor (U.S. Patent 7,334,262) teaches the prevention of worms through intercepting and emulating executable code (note Fig. 3).

Copeland, III (U.S. Patent Application Publication 2002/0144156) teaches identifying malicious code through profiling usual port traffic (note Abstract).

Anderson et al. (U.S. Patent Application Publication 2004/0064537) teaches worm detection at network gateways (note paragraph [0006]).

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID J. PEARSON whose telephone number is (571)272-0711. The examiner can normally be reached on Monday - Friday, 7:30am - 5:00pm; off every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. J. P./
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437